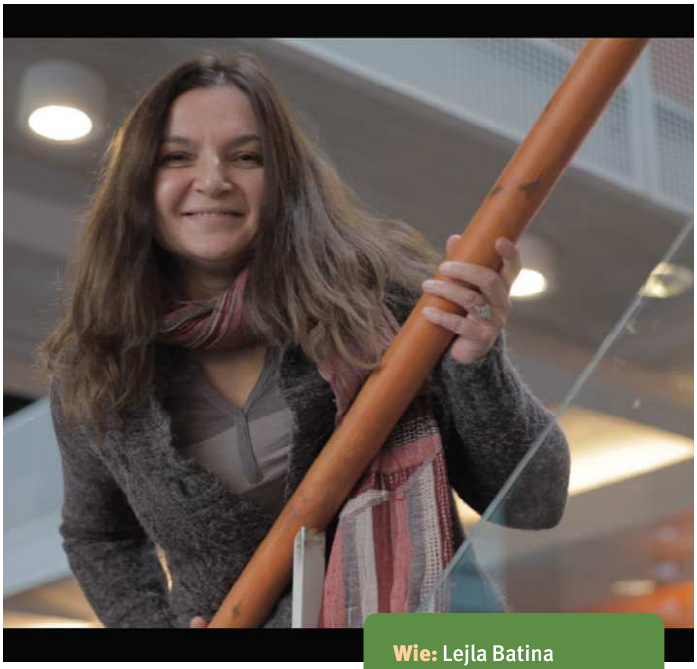
Chipkaarten beschermen tegen afluisteren

Chipkaarten en hun uitleesapparaten verklappen ongewild allerlei beveiligingsinformatie via warmte, straling en elektriciteitsverbruik.

U krijgt steeds meer chipkaarten in uw portemonnee en broekzak. Uw paspoort heeft een chip, uw treinkaart en ook uw autosleutel. Die chipkaarten zijn beveiligd met geheime sleutels. Daarmee kan een pashouder bewijzen dat hij of zij echt de echte kaart op zak heeft. Kwaadwillenden zinnen voortdurend op mogelijkheden om die geheime sleutels te stelen. Als dat lukt, kunnen ze de chips namelijk klonen. En vervolgens ergens binnenkomen met een gekopieerde toegangspas, wegrijden met een nepautosleutel of een paspoort namaken en andermans identiteit misbruiken.

Eén van de trucs die aanvallers gebruiken om geheime sleutels te stelen is het afluisteren van de fysieke signalen die een chip of uitleesapparaat onwillekeurig afgeeft, zoals straling, temperatuur of elektriciteitsverbruik. Onderzoekster Lejla Batina van de Radboud Universiteit Nijmegen gaat zich de komende vijf jaar verplaatsen in dit type aanvallers. Ze wil zoveel mogelijk verschillende aanvalsmethoden in kaart brengen. Met die kennis kan ze nieuw testgereedschap ontwikkelen waarmee gespecialiseerde bedrijven de beveiliging van nieuwe chipkaarten kunnen testen. En met een beetje geluk vindt de onderzoekster bovendien nieuwe manieren om chipkaarten te beschermen tegen dit soort afluister-aanvallen.



Wie: Lejla Batina
Waar: Nijmegen
Wat: onderzoek
Waarom: chipkaarten beveiligen

Hoe luistert iemand een pasje af?

"Een klassiek voorbeeld van zo'n 'side channel attack' is te zien in oude zwart-wit films: een inbreker gebruikt een stethoscoop om de cijfercombinatie van een kluis te raden. Hij plaatst de stethoscoop op het cijferslot en draait langzaam totdat hij het slot hoort klikken. Zo kan hij nummer voor nummer de geheime code achterhalen en de kluis kraken. Op dezelfde manier kan een digitale aanvaller bijvoorbeeld het elektriciteitsverbruik van een scan-apparaat afluisteren wanneer een klant daar een chipkaart tegenaan houdt. Er is namelijk een duidelijk verband tussen het stroomverbruik en de data die wordt verzonden. Ook uit de temperatuur van een chip valt van alles af te leiden. Wanneer er bijvoorbeeld intensief wordt gerekend, wordt de chip warmer. Dat is belangrijke informatie, die de aanvaller kan misbruiken om bijvoorbeeld het deel van de communicatie op te sporen waarin de geheime sleutel wordt verstuurd. Hoe meer signalen de aanvaller combineert, hoe dichter hij of zij bij het ontdekken van de geheime sleutel komt. Vrijwel elke week wordt er een nieuw type aanval ontdekt."

Wat gaat u onderzoeken?

"Ik ga zoveel mogelijk verschillende chipkaarten op allerlei manieren gebruiken en tegelijkertijd alle signalen meten die de kaarten en hun afleesapparaten onbedoeld uitzenden, zoals het elektriciteitsverbruik, de temperatuur en de straling. Ik werk daarbij samen met Riscure, een bedrijf dat in opdracht de beveiliging test van ingebedde apparaten door te kijken of ze die kunnen kraken. Vervolgens laat ik zelflerende software uitrekenen hoe aanvallers deze signalen slim kunnen combineren om geheime sleutels te achterhalen. Zo kan ik nieuwe aanvalsmethoden ontdekken en bestaande fine-tunen. Met die informatie kan ik de testbatterijen van Riscure en andere bedrijven perfectioneren en uitbreiden."

Hoe kun je een chipkaart beschermen?

"Eén methode om afluisteren te bemoeilijken is door ruis aan het signaal toe te voegen. Of door de informatie in brokjes en beetjes te versturen, in willekeurige volgorde en via verschillende wegen. Het uiteindelijke doel van mijn onderzoek is om chipkaarten te ontwerpen die beter beveiligd zijn en de privacy van gebruikers beter beschermen. Wanneer een betaalkaart bijvoorbeeld wordt uitgelezen dan wil je dat het apparaat alleen ziet hoeveel saldo er op de kaart staat. De verkopende partij hoeft niet te zien wat je adresgegevens zijn en welke eerdere aankopen je hebt gedaan. Ik hoop ervoor te zorgen dat ook dit soort vertrouwelijke informatie in de toekomst beter wordt afgeschermd."

Tekst: Jolein de Rooij

SITES

- cs.ru.nl/~lejla
- www.riscure.com
- www.ru.nl/ds/group/ds_section

Oproep

Doet u ook iets bijzonders met uw computer? Of hebt u een handige softwareoplossing voor uw hobby bedacht? Stuur dan een e-mail met als onderwerp **'Creatief met de computer'** naar **redactie@computeridee.nl**. Wie weet komt u ermee in Computer Idee.